

Fig. 1a

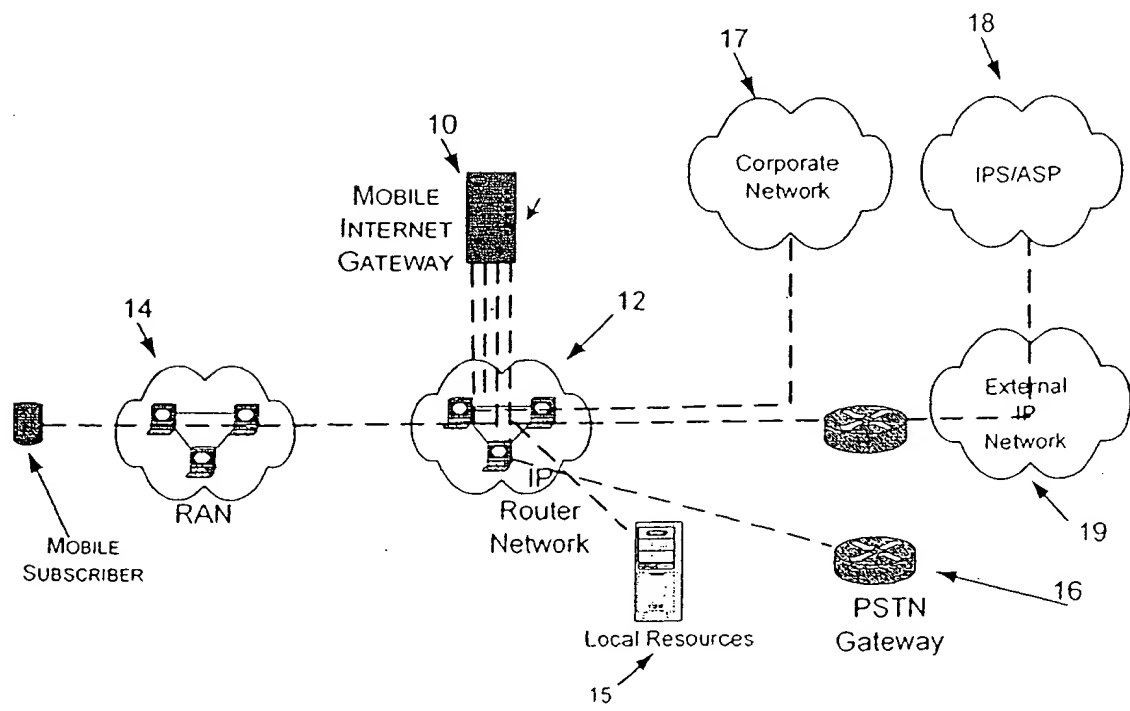


Fig. 1b

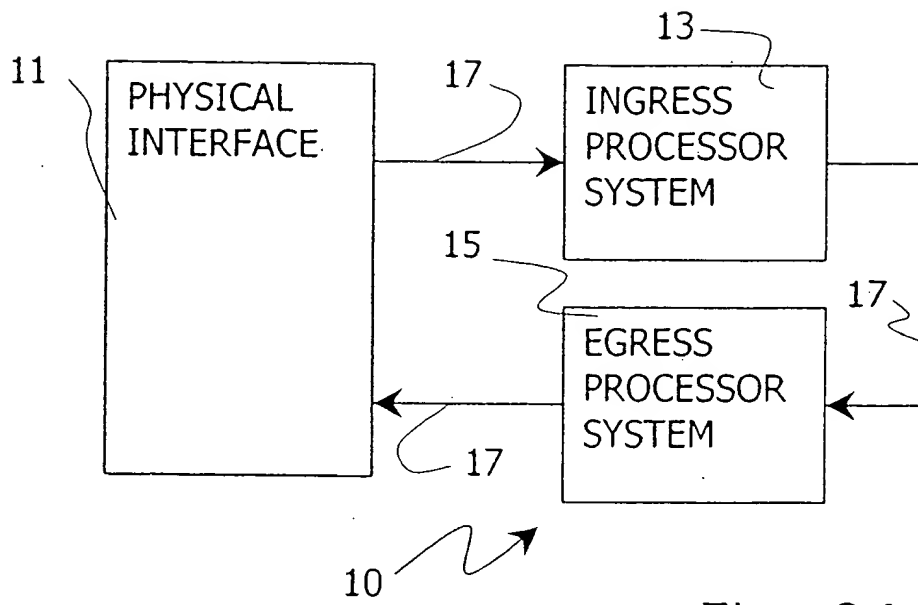


Fig. 2A

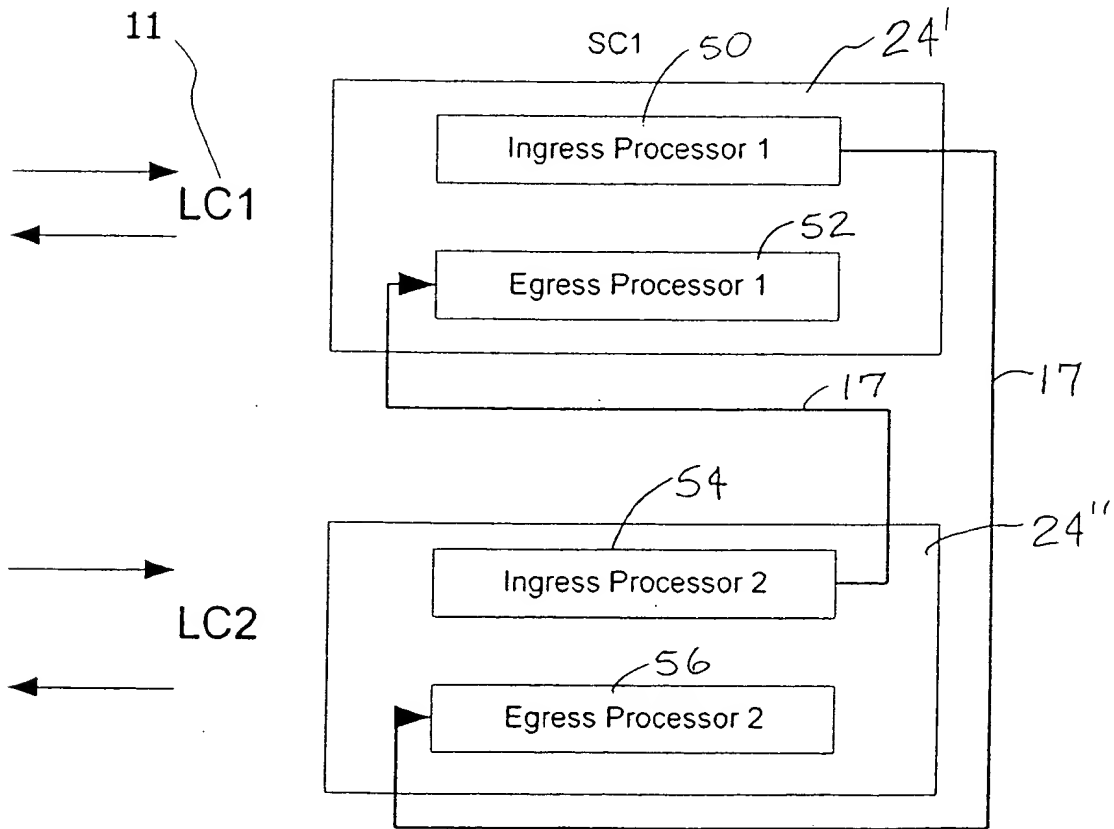


Fig. 2B

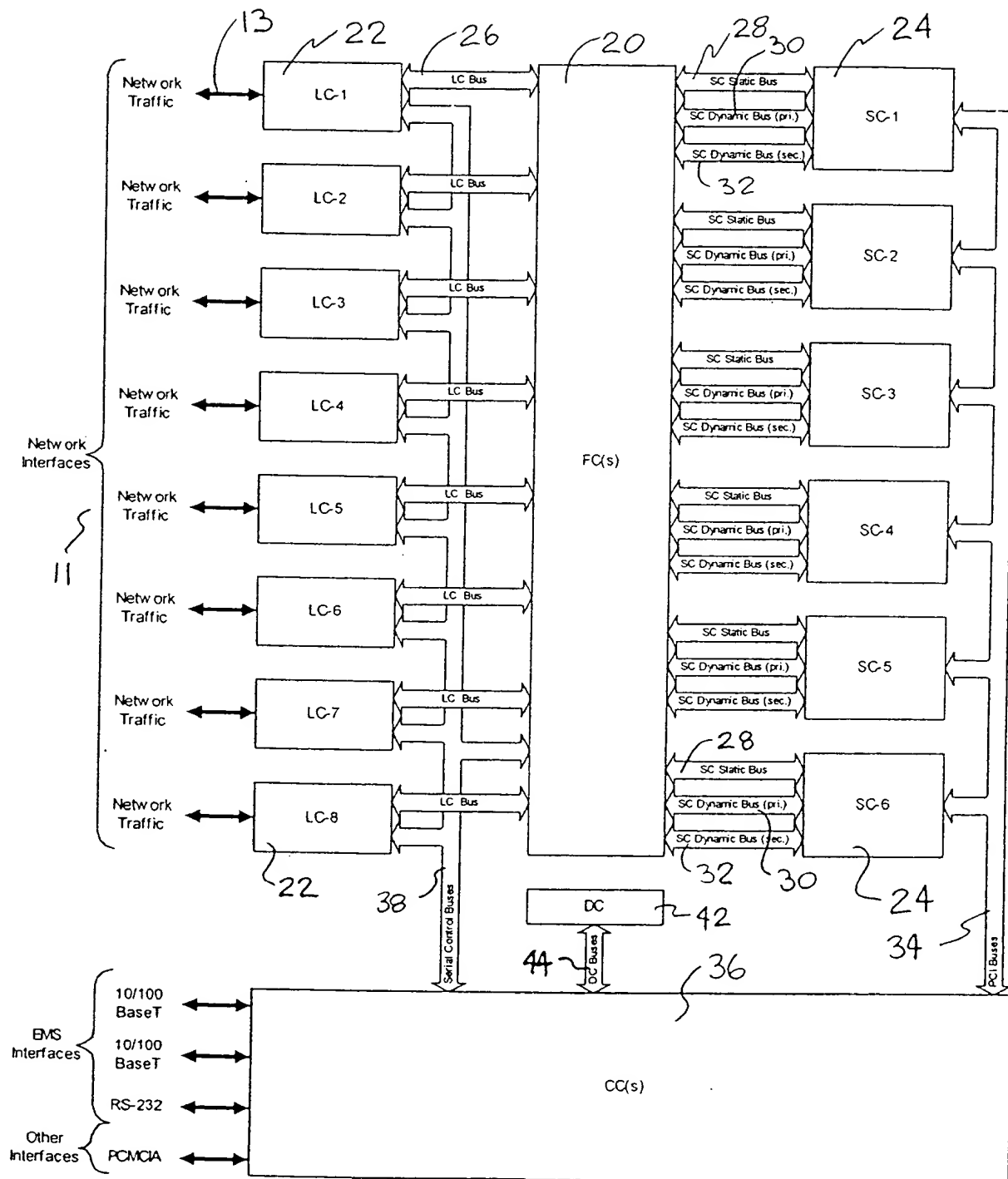


Fig. 3

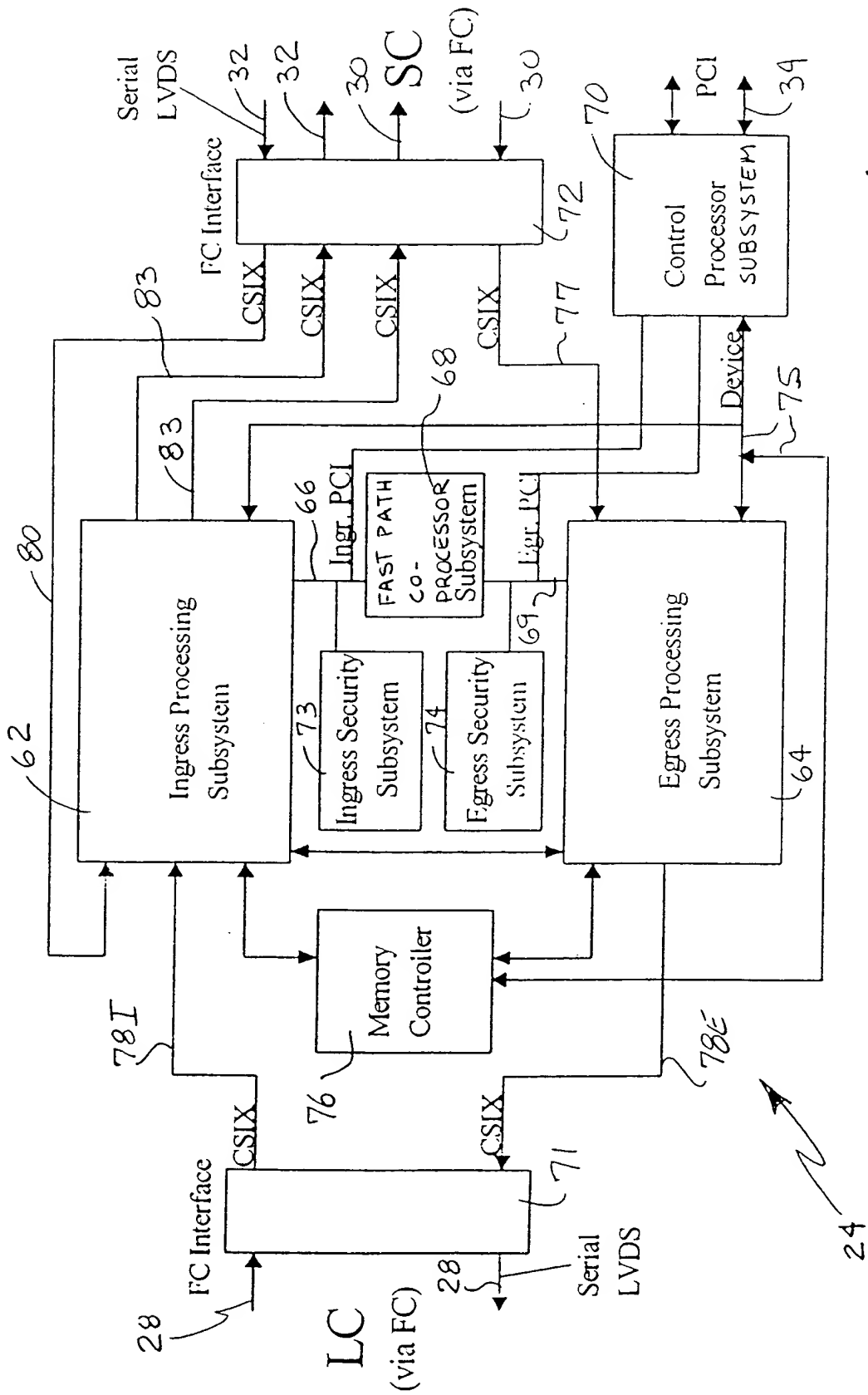


Fig. 4

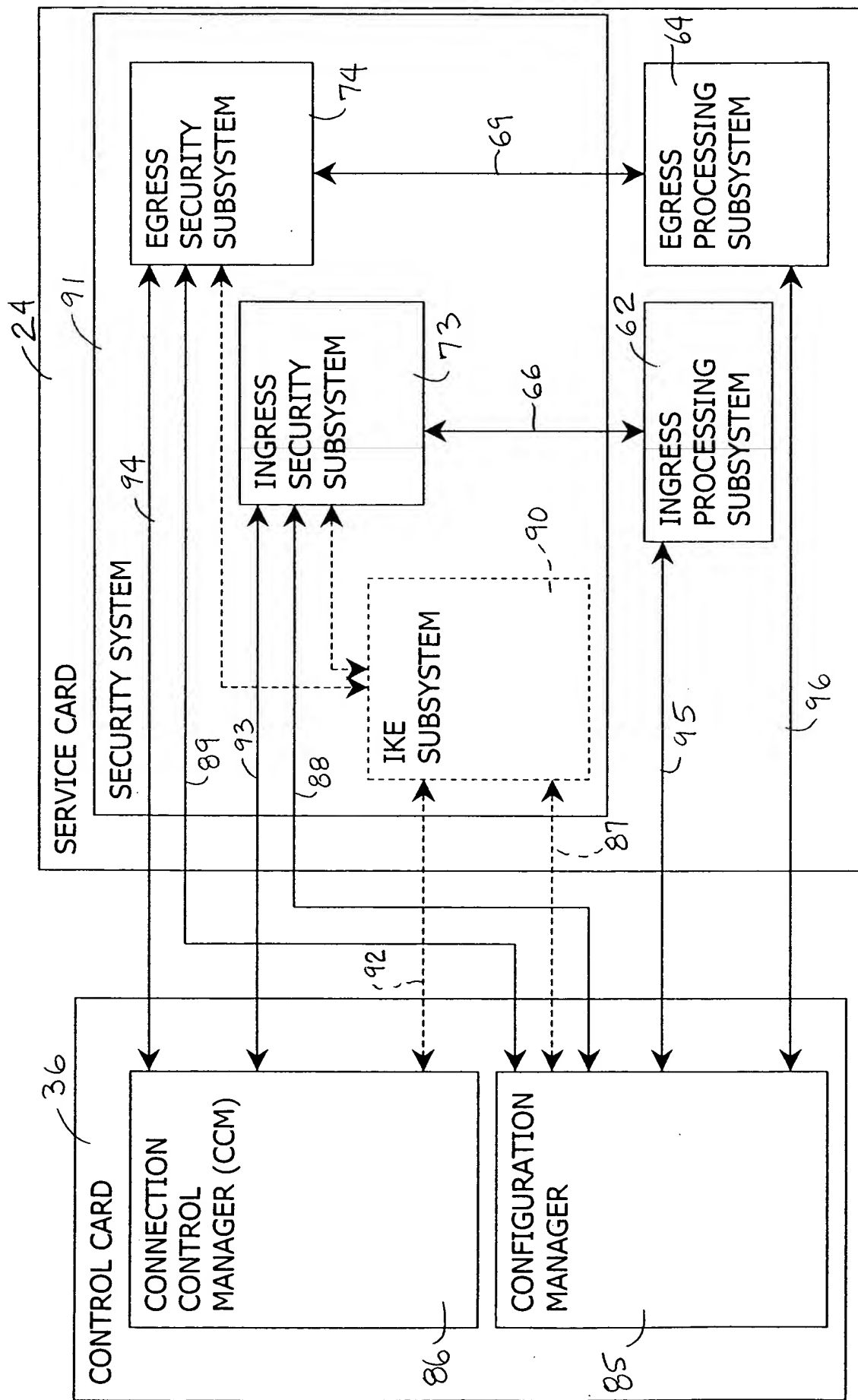


Fig. 5

The diagram illustrates a network processor architecture. At the top is the **SC Ingress Processor** (62). Below it is the **Bus Interface** (100). The **Bus Interface** connects to an **Ingress Bus** (66). The **Ingress Bus** is connected to four processing components: **Fast Path Co-Processor** (68), **Ingress Security Processor** (73), **Control Processor** (70'), and **High Speed Bridge** (70''). These components are connected to an **Egress Bus** (69). The **Egress Bus** is connected to three processing components: **Egress Processor FPGA Interface** (108), **Egress Security Processor** (74), and **Egress Network Processor Interface** (104).

Fig. 6

700  
THE TWO SECURITY ASSOCIATIONS, AT THE SECURITY SUBSYSTEMS, ESTABLISH A SHARED SECRET KEY TO BE USED FOR SYMMETRIC BLOCK ENCRYPTION (E.G., A DIFFIE-HELLMAN KEY EXCHANGE).

702  
USE ONE OF THE EGRESS SECURITY SUBSYSTEM AND INGRESS SECURITY SUBSYSTEM TO HOST THE SECURITY ASSOCIATION

704  
MAIN MODE AND QUICK MODE IKE EXCHANGES ARE PERFORMED TO ESTABLISH A SECURITY ASSOCIATION WITH A REMOTE PEER

706  
A "DELETE NOTIFICATION" MESSAGE ENCRYPTED WITH THE ISAKMP SA KEY IS CREATED AND SENT TO THE CCM ON THE CONTROL CARD

708  
THE SERVICE CARD IDENTIFIER IS RECORDED AT THE CCM, AND PEER ADDRESS FOR THE NEWLY CREATED SECURITY ASSOCIATION IS RECORDED AT THE CCM

710  
KEY, ENCRYPT SESSION DATA

712  
FORM AND SEND SECURITY MESSAGE INCLUDING AUTHENTICATION FOR AUTHENTICATING THE TRANSMISSION OF THE SESSION DATA

714  
CHECK AUTHENTICATION AT RECEIVER SUBSYSTEM

716  
DECRYPT THE SM BY THE RECIPIENT USING THE SHARED SECRET KEY OF STEP 700. THE DECRYPTED SESSION DATA IS THEN LOADED INTO THE SECURITY SUBSYSTEM TABLES.

Fig. 7A

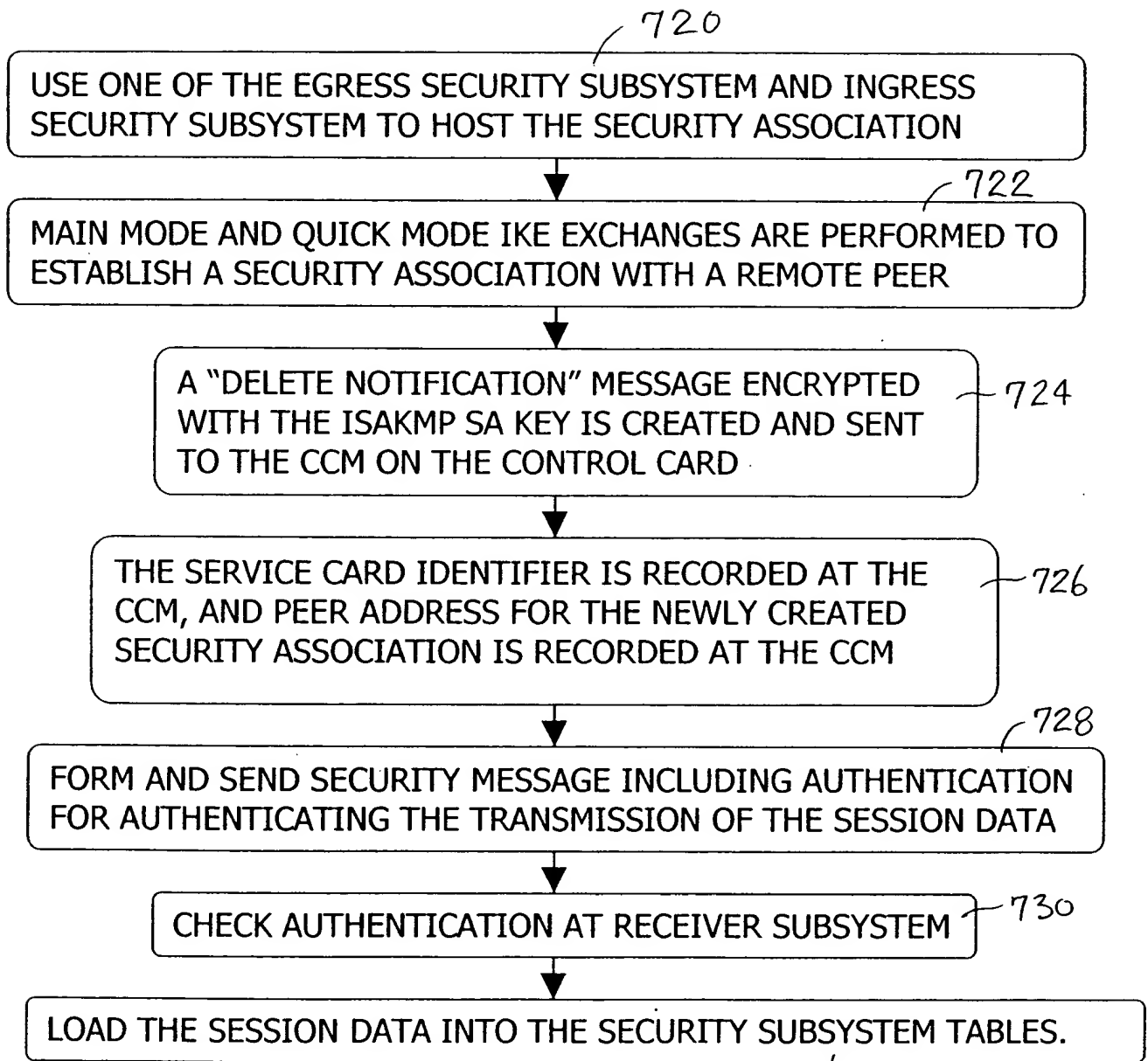


Fig. 7B



USE ONE OF THE EGRESS SECURITY SUBSYSTEM AND INGRESS SECURITY SUBSYSTEM TO HOST THE SECURITY ASSOCIATION

MAIN MODE AND QUICK MODE IKE EXCHANGES ARE PERFORMED TO ESTABLISH A SECURITY ASSOCIATION WITH A REMOTE PEER

A "DELETE NOTIFICATION" MESSAGE ENCRYPTED WITH THE ISAKMP SA KEY IS CREATED AND SENT TO THE CCM ON THE CONTROL CARD

THE SERVICE CARD IDENTIFIER IS RECORDED AT THE CCM, AND PEER ADDRESS FOR THE NEWLY CREATED SECURITY ASSOCIATION IS RECORDED AT THE CCM

FORM AND SEND SECURITY MESSAGE

LOAD THE SESSION DATA INTO THE SECURITY SUBSYSTEM TABLES.

Fig. 7C

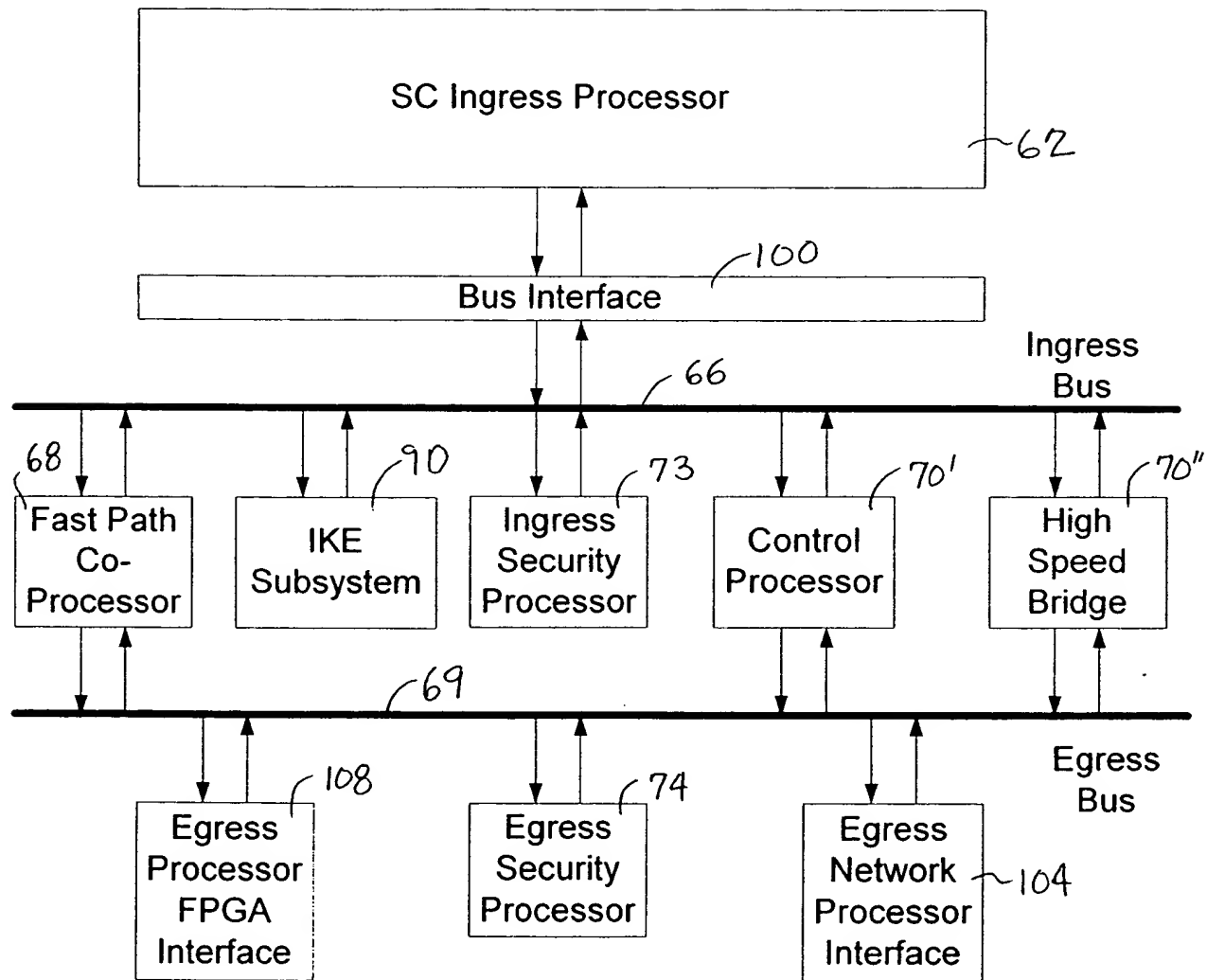


Fig. 8